New security analysis for UOV-based signature candidates with small public key size

*Yasuhiko Ikematsu (Kyushu University)
Hiroki Furue (NTT)
Rika Akiyama (NTT)

5th NIST PQC Standardization conference

April 11, 2024

Institute of Mathematics for Industry
Kyushu University

Overview of our result

① Rectangular MinRank attack is applicable to UOV variants

- MAYO and QR-UOV are secure under RM attack
- Initial parameters of VOX are not secure under RM attack
  (H. Guo et al. improved RM attack against VOX in the previous talk)

② Some parameters of SNOVA are not secure
  (P. Li and J. Ding obtained a similar result in their paper of this conference)

- The construction can be explained without matrix ring
- SNOVA has a small UOV construction than expected
- Some attacks against SNOVA can be improved
  (i.e. KS attack, Reconciliation attack and Intersection attack)

In this talk, we focus on SNOVA

Contents

§1.1 Construction of UOV[KPG]

- Parameters $v, o, q \in \mathbb{N}$, $n := v + o$, $\mathbb{F}_q$: finite field

$x' = (x_1, \ldots, x_v)$, $x'' = (x_{v+1}, \ldots, x_{v+o})$, n-variables

vinegar variables　　oil variables　　$x = (x', x'')$

- UOV central map

$$f_1(x_1, \ldots, x_v, x_{v+1}, \ldots, x_n) = \sum_{1 \le i,j \le v} a_{i,j}^{(1)} x_i x_j + \sum_{1 \le i \le v, 1 \le j \le o} a_{i,v+j}^{(1)} x_i x_{v+j}$$

$$\vdots$$

$$f_o(x_1, \ldots, x_v, x_{v+1}, \ldots, x_n) = \sum_{1 \le i,j \le v} a_{i,j}^{(o)} x_i x_j + \sum_{1 \le i \le v, 1 \le j \le o} a_{i,v+j}^{(o)} x_i x_{v+j}$$

(Each coefficient is randomly chosen from $\mathbb{F}_q$)

- UOV secret key

$$F := (f_1, \ldots, f_o) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^o$$

$S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$　　invertible linear map on $\mathbb{F}_q^n$

- UOV public key

$$P := F \circ S = (p_1, \ldots, p_o) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^o$$

[KPG] Kipnis, A., Patarin, L., Goubin, L.: “Unbalanced Oil and Vinegar Schemes”, EUROCRYPT 1999

§1.2 Matrix representation

Secret key: $F = (f_1, \dots, f_o), S$ Public key: $P = F \circ S = (p_1, \dots, p_o)$

vinegar variables

oil variables

$$f_1(x_1, \dots, x_n) = (x_1 \ \cdots x_v \ \ x_{v+1} \cdots \ x_n) \begin{pmatrix} a_{11}^{(1)} & \cdots & a_{1v}^{(1)} & a_{1,v+1}^{(1)} & \cdots & a_{1n}^{(1)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{v1}^{(1)} & \cdots & a_{vv}^{(1)} & a_{v,v+1}^{(1)} & \cdots & a_{vn}^{(1)} \\ a_{v+1,1}^{(1)} & \cdots & a_{v+1,v}^{(1)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}^{(1)} & \cdots & a_{nv}^{(1)} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} = F_1$$

$$\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots$$

$$f_o(x_1, \dots, x_n) = (x_1 \ \cdots x_v \ \ x_{v+1} \cdots \ x_n) \begin{pmatrix} a_{11}^{(o)} & \cdots & a_{1v}^{(o)} & a_{1,v+1}^{(o)} & \cdots & a_{1n}^{(o)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{v1}^{(o)} & \cdots & a_{vv}^{(o)} & a_{v,v+1}^{(o)} & \cdots & a_{vn}^{(o)} \\ a_{v+1,1}^{(o)} & \cdots & a_{v+1,v}^{(o)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}^{(o)} & \cdots & a_{nv}^{(o)} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} = F_o$$

$$\left(Q_{p_1}, \dots, Q_{p_o}\right) = (S \cdot F_1 \cdot S^t, S \cdot F_2 \cdot S^t, \dots, S \cdot F_o \cdot S^t)$$

Contents

§2.1 Idea of SNOVA

- UOV central map

$$f_k(x_1, \ldots, x_n) = \sum_{1 \le i,j \le v} a_{i,j}^{(k)} x_i x_j + \sum_{1 \le i \le v, 1 \le j \le o} a_{i,v+j}^{(k)} x_i x_{v+j}$$

- Idea of SNOVA: Change all components to matrices !

- SNOVA central map $\quad l \in \mathbb{N}$

$$f_k(X_1, \ldots, X_n) = \sum_{1 \le i,j \le v} X_i \cdot A_{i,j}^{(k)} \cdot X_j^t + \sum_{1 \le i \le v, 1 \le j \le o} X_i \cdot A_{i,v+j}^{(k)} \cdot X_{v+j}^t$$

- Each $X_h = (x_{i,j}^{(h)})$ is an $l \times l$ variable matrix, each $A_{i,j}^{(k)}, A_{i,v+j}^{(k)}$ is an element of $M_l(\mathbb{F}_q)$

§2.2 Central map of SNOVA

$v, o, l \in \mathbb{N}, n := v + o$

F_1

$$f_1(X_1, \ldots, X_n) = (X_1 \ \cdots X_v \ X_{v+1} \cdots X_n) \begin{pmatrix} A_{11}^{(1)} & \cdots & A_{1v}^{(1)} & A_{1,v+1}^{(1)} & \cdots & A_{1n}^{(1)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ A_{v1}^{(1)} & \cdots & A_{vv}^{(1)} & A_{v,v+1}^{(1)} & \cdots & A_{vn}^{(1)} \\ A_{v+1,1}^{(1)} & \cdots & A_{v+1,v}^{(1)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ A_{n1}^{(1)} & \cdots & A_{nv}^{(1)} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} X_1^t \\ \vdots \\ X_v^t \\ X_{v+1}^t \\ \vdots \\ X_n^t \end{pmatrix}$$

$\vdots$

$$f_o(X_1, \ldots, X_n) = (X_1 \ \cdots X_v \ X_{v+1} \cdots X_n) \begin{pmatrix} A_{11}^{(o)} & \cdots & A_{1v}^{(o)} & A_{1,v+1}^{(o)} & \cdots & A_{1n}^{(o)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ A_{v1}^{(o)} & \cdots & A_{vv}^{(o)} & A_{v,v+1}^{(o)} & \cdots & A_{vn}^{(o)} \\ A_{v+1,1}^{(o)} & \cdots & A_{v+1,v}^{(o)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ A_{n1}^{(o)} & \cdots & A_{nv}^{(o)} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} X_1^t \\ \vdots \\ X_v^t \\ X_{v+1}^t \\ \vdots \\ X_n^t \end{pmatrix}$$

F_o

- Each F_k is an element of $M_n\left(M_l(\mathbb{F}_q)\right)$
- However, we have $M_n\left(M_l(\mathbb{F}_q)\right) = M_{ln}(\mathbb{F}_q)$

§2.3 Ring UOV (pre-construction)

- Secret key: $F_1, \ldots, F_o \in M_{ln}(\mathbb{F}_q), S \in GL_{ln}(\mathbb{F}_q)$
- Public key: $G_1 = S \cdot F_1 \cdot S^t, \ldots, G_o = S \cdot F_o \cdot S^t$
- Verification key: $P_1(X) = X \cdot G_1 \cdot X^t$

$\vdots$

$P_o(X) = X \cdot G_o \cdot X^t$

$X \coloneqq (X_1 \cdots X_v \; X_{v+1} \cdots X_n)$
$l \times ln$ variable matrix

$l^2 o$ quad poly in $l^2 n$ variables

$$P \coloneqq (P_1, \ldots, P_o) : M_l(\mathbb{F}_q)^n \longrightarrow M_l(\mathbb{F}_q)^o$$

- Each public matrice G_k generates l^2 polynomials
  → It reduces SNOVA public key size
- The quad poly obtained are sparse, so they look like vulnerable
  (In fact, there is a polynomial-time forgery attack for Ring UOV. See our report.)

§2.4 SNOVA construction

■ Verification key:

$$P_k(X) = X \cdot G_k \cdot X^t$$

As a countermeasure,
P_k was made to be complex

$$P_k(X) = \sum_{i=1}^{l^2} A_i \, X \cdot Q_{i1} G_k Q_{i2} \cdot X^t \, B_i$$

- Here, A_i, B_i, Q_{i1}, Q_{i2} are generated as public matrices
- In verification, P_k is computed from $\{G_k, A_i, B_i, Q_{i1}, Q_{i2}\}$

compressed as a seed

§2.5 Remark

For Sign and Ver, some conditions are required.

- Secret key: $F_1, \ldots, F_o \in M_{ln}(\mathbb{F}_q), S \in GL_{ln}(\mathbb{F}_q)$

$$S \in GL_n(\mathcal{A}) \subset GL_{ln}(\mathbb{F}_q)$$
$$\mathcal{A} \subset M_l(\mathbb{F}_q) \quad l\text{-dim subfield}$$

- Public key: $G_1 = SF_1S^t, \ldots, G_o = SF_oS^t$

$$\{G_1, \ldots, G_o, A_i, B_i, Q_{i1}, Q_{i2}\}$$

- Verification key:

Q_{i1}, Q_{i2} are chosen to be commutative with S

$$P_k(X) = \sum_i A_i\, X \cdot Q_{i1} G_k Q_{i2} \cdot X^t\, B_i$$

Contents

§3.1 Security analysis

Matrix ring over matrix ring = matrix ring

$$M_n\left(M_l(\mathbb{F}_q)\right) = M_{ln}\left(\mathbb{F}_q\right)$$

⇒ Public key $G_1, \ldots, G_o$ are UOV with parameter (lv, lo)

✓ In the document, SNOVA was considered as UOV with (l^2v, l^2o)

We can apply some key recovery attacks

⇒
- Kipnis-Shamir attack[KS]
- Reconciliation attack[D08]
- Intersection attack[B21]

[KS] Kipnis et al., Cryptanalysis of the Oil and Vinegar signature scheme, CRYPTO'98
[D08] Ding et al., New differential-algebraic attacks and reparametrization of rainbow, ACNS 2008
[B21] W. Beullens, "Improved cryptanalysis of UOV and Rainbow", EUROCRYPT 2021

§3.2 Security analysis 2

- $T, T' \in \mathcal{A},\ \Lambda_T := \begin{pmatrix} T & & \\ & \ddots & \\ & & T \end{pmatrix} \in M_{ln}(\mathbb{F}_q)$

$$\Lambda_T G_k \Lambda_{T'}^t = \Lambda_T S F_k S^t \Lambda_{T'}^t = S\left(\Lambda_T F_k \Lambda_{T'}^t\right) S^t$$

has the same oil space as G_k

- $T_1, \ldots, T_l \in \mathcal{A}$ basis

$\Lambda_{T_i} G_k \Lambda_{T_j}^t \ (1 \le i, j \le l, 1 \le k \le o)$

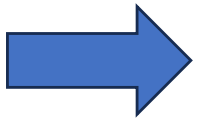
are UOV with parameter (lv, lo)

Target matrices $\{G_1, \ldots, G_o\} \Rightarrow \left\{\Lambda_{T_i} G_k \Lambda_{T_j}^t\right\}_{(1 \le i, j \le l, 1 \le k \le o)}$

§3.3 Complexity reduction

- Kipnis-Shamir attack

$$q^{l^2v-l^2o}$$

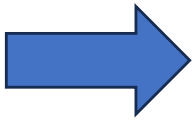


$$q^{lv-lo}$$

- Reconciliation attack

MQ problem with l^2v variables and l^2o quadratic equations/$\mathbb{F}_q$

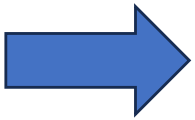
$$MQ(l^2v, l^2o)$$



$$MQ(lv, l^2o)$$

- Intersection attack $(v < 2o)$

$$MQ(2l^2v - l^2o + 1, 3l^2o - 2)$$



$$MQ(2lv - 2o + 1, 4l^2o - 2)$$

§3.4 Complexity estimation

Security category	Parameter (v, o, l)	Kipnis-Shamir		Reconciliation		Intersection	
		old	new	old	new	old	new
	(28,17,2)	181	**93**	-	**132**	275	**87**
	(25,8,3)	617	209	-	209	819	221
	(24,5,4)		309	-	270	1439	349
	(43,25,2)		**149**	-	**193**	439	**120**
	(49,11,3)		461	-	438	1631	529
	(37,8,4)				388		
	(61,33,2)	453	**229**	-	277	727	**167**
	(66,15,3)	1841	617	-	575	2178	690
	(60,10,4)	3205	805	-	695	3602	922

- ✓ Each complexity is evaluated in gate count
- ✓ Level I=143 gates, Level II=207 gates, Level III=272 gates
- ✓ **Parameters for $l = 2$ do not satisfy the security level**

Conclusion in this talk

- SNOVA is originally constructed by using matrix ring
- The construction can be explained without matrix ring
- SNOVA has a small UOV construction
- Some attacks against SNOVA can be improved
- Parameters for $l = 2$ do not satisfy the security level

Thank you!

Institute of Mathematics for Industry
Kyushu University

Kyushu University, IMI
Yasuhiko Ikematsu
ikematsu@imi.kyushu-u.ac.jp